Addressing security challenges in copyright management applications: the blockchain perspective

Nour El Madhoun, Badis Hammi, Saad El Jaouhari, Djamel Mesbah, Elsi Ahmadieh

Addressing Security Challenges in Copyright Management Applications: The Blockchain Perspective

Nour El MADHOUN*, Badis HAMMI†, Elsi AHMADIEH‡
*LISITE Laboratory, ISEP, 10 Rue de Vanves, Issy-les-Moulineaux, 92130, France
Sorbonne Université, CNRS, LIP6, 4 place Jussieu 75005 Paris, France
nour.el-madhoun@isep.fr
† SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, France
badis.hammi@telecom-sudparis.eu
‡Lebanese University, Faculty of Technology, Department Communications and Computer Networks Engineering, Beirut, Lebanon
elsiahmadieh@gmail.com

***Abstract*—Today, the field of copyright management faces several security vulnerabilities, making it a target for various types of rights violations, including piracy and unauthorized use of creative works. In this context, blockchain technology has emerged as a robust solution in this sector as it offers enhanced security, trust for creators, and increased transparency. In this paper, we first present an overview of the four main applications in the field of copyright management: (1) management of licenses and royalties, (2) market for artworks, (3) registration and protection of works, and (4) proof of anteriority. We then analyze in details the critical security vulnerabilities of these applications. Subsequently, we explain how blockchain technology can be used to mitigate these vulnerabilities. Finally, we discuss possible methods of preventing common blockchain-based attacks in these copyright management applications.**

***Index Terms*—Artwork, Attack, Blockchain Technology, Copyright, NFT, Proof of Anteriority, Proof of Ownership, Royalties, Security.**

I. Introduction

The copyright management sector is currently facing a series of security vulnerabilities that pose significant risks to the protection and enforcement of copyrights. These issues make the sector particularly exposed to various types of infringements, such as piracy and unauthorized use of creative works. As a result, these threats seriously compromise the legitimate rights of authors and the originality of works, while endangering the integrity of artistic and intellectual creation [1]–[3].

Blockchain technology has recently emerged as a key and robust solution to a variety of security challenges in several sectors, particularly in the copyright management sector. An essential element of this technology is smart contracts which represent decentralized and autonomous programs that automatically execute on the blockchain when predefined conditions are met (more details on blockchain and smart-contracts technologies can be found in [4]–[8]). Indeed, thanks to the intrinsic properties of the blockchain technology such as decentralization, immutability, and transparency, along with the principle of smart contracts, several significant advantages are provided. These include enhanced copyright security, protection against unauthorized modifications, complete traceability of operations, and boosted confidence among creators and industry professionals [9]–[11].

We summarize the contributions of this paper as follows. (1) we provide an overview of the four main copyright management applications (Section II). (2) we analyze the critical security vulnerabilities in these applications (Section III). (3) we highlight how the blockchain technology could counter these security vulnerabilities (Section IV). And (4) we discuss the different strategies to prevent the most common attacks on blockchain technology in the context of the discussed copyright management applications (Section V).

II. Overview of the Main Copyright Management Applications

Blockchain technology can ensure the security of numerous applications in the field of copyright management. This paper focuses on the four main applications in the latter field: (1) management of licenses and royalties, (2) market for artworks, (3) registration and protection of works, and (4) proof of anteriority. In this section, we present an overview of how these applications are conventionally implemented, excluding the integration of blockchain technology.

A. Management of Licenses and Royalties

The management of licenses and royalties is traditionally a complex and centralized process. It involves contractual agreements between the creators of works such as authors, musicians, artists, and so on, and entities wishing to use these works. These contracts define the conditions of use, covering aspects like the duration of the license, the geographical areas concerned, and the types of authorized use (e.g., broadcasting, reproduction, public display, and so on). Typically, the transactions and rights management are handled by intermediaries, such as copyright agencies or collective management

organizations. They are responsible for negotiating the terms of licenses, collecting royalties from users (e.g., publishers, broadcasters, or online platforms), and redistributing them to the rights-holders based on the established agreements. The systems used to manage these processes are based on centralized databases that record details of works, contracts, uses, and financial transactions. They aim to accurately track the use of works in order to calculate the royalties due. Additionally, they seek to efficiently manage licensing agreements and payments while ensuring that creators receive fair compensation for the use of their works [12], [13].

B. Market for Artworks

In the traditional market for artworks, transaction management and authenticity verification are primarily ensured by art galleries, auction houses, and online platforms. These intermediaries have a key role in connecting artists with buyers and facilitating the sale and purchase of works. Indeed, verifying the provenance and authenticity of works, a task carried out by field experts, is essential for buyers and sellers to ensure the value and legitimacy of the exchanged works. However, this centralized model inherently presents complex aspects. For instance, reliance on experts for verification procedures can limit the process's speed and accessibility. Furthermore, centralized structures may introduce additional costs for artists and buyers due to commissions and management fees. Finally, centralizing these operations involves logistical challenges such as secure storage and transportation of works, as well as managing the confidential information of customers and transaction details [14].

C. Registration and Protection of Works

The registration and protection of works are traditionally managed by specialized intellectual property organizations. These organizations provide a legal framework for the registration of works, enabling creators to obtain official recognition and proof of their ownership. The registration process involves creators submitting detailed information about their work, including the title, a full description, and often a copy or an extract of the work. Once the work is registered, it is added to a public register, which offers transparency and facilitates the resolution of potential copyright disputes. This system represents a crucial element in the protection of creators' rights, enabling them to legally assert their rights in case of violation. However, its effectiveness can vary depending on the jurisdiction and the particular nature of the work. Moreover, although registration offers some proof of anteriority, demonstrating the work's existence at a specific point in time can pose challenges. This proof is indeed essential in cases where the originality or the priority of creation of the work is under dispute. In such situations, creators may be required to provide additional evidence, such as drafts, correspondence, or testimonials to substantiate their claims, thereby highlighting the importance of documenting and safeguarding reliable proof of the creation of the work (see Section III-C) [15], [16].

D. Proof of Anteriority

The proof of anteriority often involves depositing creations with specialized organizations, or using testimonials and dated documents. This process aims to establish the existence of a work at a given point in time, especially in the case of copyright disputes. In order to prove anteriority, creators can produce various types of documents, such as drafts, correspondence, or recordings, that attest to the date of creation of the work. Sometimes, it is also possible to rely on testimonials or public records to strengthen ownership claims. These methods of proof are intended to provide legal certainty regarding the originality and ownership of the work, but the quality and reliability of any provided proof are crucial. The proofs must be clear, coherent, and convincing to withstand contestations and divergent interpretations that can arise in legal proceedings. So, although these methods are widely used due to their effectiveness in providing legal proof, they require meticulous attention to the documentation and preservation of relevant evidence to effectively support copyright claims (see Section III-D) [17] [18].

III. Security Vulnerabilities in the Main Copyright Management Applications

In this section, we analyze the security of the four main applications of copyright management introduced in the previous Section II. We present the security vulnerabilities identified in these applications as follows:

A. Vulnerabilities on the Management of Licenses and Royalties

Centralized data management: the management of licenses and royalties traditionally relies on centralized databases managed by intermediaries or institutions. These databases store all data related to copyrights, transactions, and royalty payments. Such centralization creates single points of failure where all information and associated operations can be vulnerable, potentially resulting in data loss, leaks of confidential information, or service interruptions if the central system is compromised (e.g., following a cyberattack). In addition, reliance on a centralized entity can lead to bottleneck problems where delays in data processing affect the speed and efficiency of transactions. Finally, centralization can also limit system resilience and adaptability in response to rapid market changes or regulatory requirements [19] [20].

Lack of transparency in royalty calculation and distribution: the processes for calculating and distributing royalties due to creators are often opaque in the classic systems for management of licenses and royalties. In general, both creators and rights-holders have limited visibility of how royalties are calculated, particularly regarding the actual use of their works. This opacity can result from the complexity of licensing agreements, the use of undisclosed calculation formulas, or the absence of detailed information on sales and uses of works. This situation can lead to a lack of trust for creators, who may

feel underpaid or poorly informed about the exploitation of their works. Moreover, in the absence of transparency, errors in the distribution of royalties, whether accidental or fraudulent, are difficult to detect and correct, which can lead to disputes and prolonged conflicts between the involved parties [2] [21].

Delays in payment distribution: they are often due to the complexity of the administrative processes involved in collecting, calculating, and distributing royalties. Centralized systems may require multiple verification and approval steps, prolonging the time between the collection of royalties and their distribution to creators. In addition, reconciling accounts and processing financial transactions across different institutions and jurisdictions can add further layers of complexity and delays. These delays can have a negative impact on creators, particularly independent artists or small publishers, for whom these payments may represent a significant proportion of their revenues [2] [22] [23].

Challenges in tracking all instances of work usage: conventional systems managing licenses and royalties encounter complexity in tracking and recording the use of works across various platforms and formats, particularly in the current digital context where works can be easily copied, shared, and distributed. Although these systems are often equipped with tracking mechanisms, they are not always able to thoroughly detect and document each instance of use, especially unauthorized or informal uses, such as those on social media, streaming platforms, or via illegal downloads. This shortcoming makes it difficult for right-holders to receive all the royalties due to them and opens the door to major financial losses. Furthermore, the limited ability of these systems to provide an accurate and comprehensive tracking of the use of works hampers the transparency and fairness of the distribution of royalties, posing significant challenges for both creators and distributors [24]–[26].

B. Vulnerabilities Related to the Market for Artworks

Authenticity and provenance of artworks: the authenticity and provenance of artworks represent a fundamental challenge in the traditional market for artworks. Authenticating an artwork involves verifying that it was actually created by the artist in question, and provenance concerns the history of the ownership of that artwork. Indeed, authentication and provenance often rely on physical documents such as certificates of authenticity or sales histories, which are subject to errors, omissions, or even falsifications. This creates risks for buyers, who may acquire artworks that are either inauthentic or have uncertain histories. The difficulty of reliably tracing the complete history of an artwork can also affect its market value and perceived legitimacy [27] [28].

Counterfeiting and unauthorized duplication: with modern reproduction technologies, it has become easier to create high-quality reproductions (copies) of artworks that can be difficult to distinguish from the originals. This poses a problem for buyers who may end up with a counterfeit, and also for artists and creators who may see their rights and potential revenue compromised by such illegal reproductions. In addition, unauthorized duplication can saturate the market, reducing the perceived value of the originals. This vulnerability particularly affects the market for digital artworks, where the copying and distribution of digital files is relatively easy to achieve without loss of quality [29] [30].

C. Vulnerabilities on the Registration and Protection of Works

Complexity in proving ownership and anteriority: determining proof of ownership and anteriority of a work can be complex in the traditional systems of registration and protection of works. In order to prove ownership, creators must often provide substantial evidence of their efforts to create the work, which may include drafts, correspondence, or other forms of documentation. The proof of anteriority, which involves demonstrating that a work was created at a specific point in time, can be even more difficult to establish. It generally requires tangible evidence, such as dated recordings or testimonials. Such evidence can be hard to preserve reliably over long periods and can be subject to contestation, especially if the documents are altered or lost [31] [32].

Lack of universal registers between different countries: each country has its own system for the registration and protection of works, with distinct standards, procedures, and legal requirements. This disparity creates many challenges for creators seeking to protect their works internationally. Differences in registration systems can lead to inconsistencies in copyright recognition and complicate the protection of works across national borders. These differences can limit the effectiveness of copyright protection in a globalized context where works are easily accessible and distributed around the world [33].

D. Vulnerabilities Related to the Proof of Anteriority

Dependence on physical proofs that can be altered or lost: the dependence of the proof of anteriority on several documents or physical objects such as manuscripts, drawings, recordings, or testimonies presents several vulnerabilities. Firstly, physical proofs can be altered, intentionally or accidentally, undermining their reliability. Modifications or falsifications can be made to the original documents, making it difficult to determine the authentic state of the work at any given time. Secondly, physical proofs are subject to deterioration and loss. Over time, documents can become damaged or illegible, and there is always a risk of loss due to natural catastrophes, accidents, or negligence. These factors compromise the ability of such evidence to reliably and enduringly establish the date of creation of a work [34] [35].

Difficulty in establishing incontestable proof of anteriority: in order to consider a proof of anteriority as incontestable, it needs to be not only accurate and reliable but also recognized and accepted by all the involved parties, including in a judicial context. Traditional methods of proving anteriority, such as legal deposits or testimonials, can be subject to contestation and differing interpretations. For example, questions may arise concerning the authenticity of presented documents, the credibility of witnesses, or the integrity of recordings. Additionally, in an international context, different countries may have varying standards and practices for the proof of anteriority, complicating the mutual recognition of such proofs. This situation can lead to prolonged litigation and judicial uncertainty, making it difficult to defend copyrights on an international stage [36] [37].

IV. Securing Copyright Management Applications with Blockchain Technology

In this section, we present how blockchain technology can contribute to address the ten security vulnerabilities presented in the previous Section III:

Addressing centralized data management: blockchain technology offers a solution to this vulnerability thanks to its decentralized and distributed architecture where data relating to copyrights, transactions, and payment of royalties are no longer stored in a centralized database, but are distributed across a network of blockchain nodes. Each node in the network holds a copy of the entire blockchain, guaranteeing data availability and integrity even in the case of failure of one or more nodes. This approach eliminates single points of failure and significantly reduces the risk of data loss, leaks of confidential information, and service interruptions due to cyberattacks. In addition, decentralization facilitates greater system agility and adaptability to rapid market and regulatory changes, while resolving the problems of bottlenecks associated with centralization and thus improving the speed and efficiency of copyright transactions [38] [39].

Addressing the lack of transparency in royalty calculation and distribution: the use of smart contracts on the blockchain provides a solution to this vulnerability. These contracts, once programmed and deployed on the blockchain, enable the automation of the process of calculating and distributing royalties in a reliable and transparent way. Each transaction or use of a work is immutably recorded on the blockchain, providing complete and real-time visibility on the actual use of the works. This traceability makes it possible to precisely calculate the royalties due according to the specific terms of each license agreement, thus eliminating the uncertainties and errors associated with opaque calculation formulas. In addition, thanks to the use of smart contracts, payments can be automatically initiated once the terms of the contract are met, ensuring a rapid and equitable distribution of royalties to creators. This approach promotes a greater degree of transparency for all parties involved and contributes to strengthening trust between creators, rights-holders, and users, while simplifying administration and reducing the possibility of disputes relating to the distribution of royalties [39].

Addressing delays in payment distribution: the decentralized architecture of blockchain technology facilitates direct transactions and automates payment processes through the use of smart contracts. These contracts aim to eliminate the intermediate verification and approval steps usually associated with centralized systems, enabling fast and efficient distribution of royalties to creators. Moreover, blockchain technology ensures transparent reconciliation of accounts in real time by streamlining processing times for financial transactions between different institutions and jurisdictions. This method accelerates the flow of revenue to artists and publishers, particularly those who are independent or small-scale, while improving their financial stability [40].

Addressing the tracking of instances of work usage: the combination of blockchain technology with advanced analysis tools significantly improves the traceability of works across a multitude of digital platforms. This enables real-time tracking of the use of works, whether shared on social networks, distributed via streaming platforms, or downloaded illegally. Each instance of use can be recorded on the blockchain, providing a detailed and unalterable history. This enhanced traceability assures that right-holders receive fair compensation for each use of their work, while minimizing financial losses due to unauthorized use. Indeed, this method increases transparency and fairness in the distribution of royalties, effectively addressing the major challenges faced by both creators and distributors in the current digital environment [25] [41].

Addressing the authenticity and provenance of artworks: in the market for artworks, blockchain technology can be used to create an immutable digital register that ensures the authenticity and traceability of the provenance of artworks. Each artwork registered on the blockchain is identified by a unique cryptographic identifier linked to detailed data on its origin, artist, history of ownership, and journey through the market. These details are permanently and transparently stored on the blockchain, making any falsification nearly impossible. This allows buyers to reliably and transparently verify the authenticity and provenance of an artwork, while significantly reducing the risk of acquiring inauthentic artworks or those with an uncertain history [42].

Addressing Counterfeiting and unauthorized duplication: in order to prevent counterfeiting and unauthorized duplication in the market for digital artworks, the use of NFTs (Non-Fungible Tokens) based on blockchain technology offers an innovative and effective solution. Each NFT is

a unique digital token associated with a specific artwork and serves as a certificate of ownership and digital authenticity. This uniqueness ensures that even if copies of the artwork exist, only the holder of the NFT owns the original and authenticated version. Indeed, NFTs enable transparent tracking of ownership and transactions, while making any unauthorized reproduction readily identifiable and traceable. The use of NFTs helps to preserve the value of originals and protect the rights and potential revenues of artists and creators [43].

Addressing the complexity in proving ownership and anteriority: blockchain technology simplifies proof of ownership and anteriority by offering a time-stamped, immutable registration system. When a work is registered on the blockchain, it receives a unique timestamp certifying its creation date. This information is permanently stored and cannot be altered, providing undeniable proof of the anteriority of the work. In addition, the identity of the creator can be linked to this blockchain entry, establishing a clear proof of ownership that is challenging to contest. This system also reduces the need to maintain physical proofs that are susceptible to alteration or loss and streamlines the validation process in the case of copyright disputes [44].

Addressing the lack of universal registers between different countries: blockchain technology operates as a universal ledger for the registration and protection of works, transcending national borders. Each work registered on the blockchain can be viewed from any country, enabling international recognition and protection of copyrights. This uniformity of registration helps to resolve any inconsistencies due to different national legal systems and registration procedures. Consequently, creators can benefit from a more homogeneous protection of their works around the world, making it easier to manage copyrights in a globalized context where digital works can easily cross borders [45].

Addressing the Dependence on physical proofs: blockchain technology offers a digital solution for storing all proofs of anteriority in a cryptographically secure form, where documents, records, or any other type of proof are digitized and stored as transactions in blocks. Each block is cryptographically linked to the previous one, forming an immutable, tamper-resistant chain. Consequently, any modification made to a record is immediately detectable. Additionally, blockchain technology ensures the durability of all proofs because even if physical copies are lost or damaged, their digital versions remain intact and verifiable on the chain [46] [47].

Addressing the difficulty in establishing incontestable proof of anteriority: the transparency and immutability of blockchain technology enable reliable and widely recognized proof of anteriority to be established. In fact, when a proof of anteriority is recorded on the blockchain, it is time-stamped and becomes accessible to all the involved parties. This time-stamping provides indisputable proof of the existence of the work at a given point in time. Moreover, due to the decentralized nature of blockchain, these records are independent of any central authority, which reinforces their credibility and acceptance in a judicial context. Finally, thanks to the distributed nature of blockchain, these proofs of anteriority are recognized internationally, facilitating the defense of copyright on the world stage and reducing the risk of protracted litigation [46] [47].

V. Preventing the Most Common Blockchain Attacks in Copyright Management Applications

In this section, we discuss the various prevention strategies that can be adapted to counter the most common attacks on blockchain technology (51% attack, sybil attack, routing attack, double spending attack and smart contract vulnerabilities [8], [9], [48]–[50]) in the copyright management applications (see Section II) if the blockchain technology is adopted.

Preventing the 51% attack: a 51% attack occurs when a malicious actor takes control of more than 50% of a blockchain network's computing power, enabling him to manipulate the blockchain, perform potential double-spending, or censor and rewrite transactions. Using Proof of Stake (PoS) blockchains or alternative consensus algorithms such as Proof of Authority (PoA) may make such control economically or logistically unfeasible. Additionally, implementing extra security protocols and redundant validation, such as cross-validation by independent nodes, can strengthen blockchain integrity. The increased decentralization of the network, with a wide and diverse distribution of nodes, can also reduce the probability of domination by a single group. Indeed, the introduction of strict rules for block creation and transaction validation adds an extra layer of security. Moreover, the use of hybrid blockchain networks, combining the characteristics of public and private chains, can offer additional validation and enhanced security. All these joint methods guarantee effective protection against manipulation and attacks, thereby ensuring the reliability and transparency of transactions and registrations in the field of copyright management [51] [52].

Preventing the sybil attack: in a sybil attack, a malicious actor creates multiple false identities to influence or disrupt the network. To remedy such an attack, it is necessary to adopt a robust system of authentication and verification of nodes, such as the use of consensus mechanisms that require some form of proof of identity or economic participation, as in PoS or PoA systems. The establishment of lists of approved nodes or the verification of participants by cryptographic methods, such as digital signatures, can also prevent malicious actors from creating multiple falsified identities. Indeed, continuous monitoring of the network must be maintained to quickly detect and isolate any suspicious nodes. Moreover, the use of hybrid networks, which combine features of public

and private blockchains, can increase security by restricting access to trusted nodes. These measures, when applied consistently, improve the resilience and reliability of blockchain-based copyright management applications against Sybil attacks [53]–[55].

Preventing the routing attack: a routing attack, where a malicious entity intercepts or modifies network traffic between blockchain nodes to disrupt or monitor communications, can be prevented by employing end-to-end encryption. This ensures that the transmitted data remain secure and unreadable to unauthorized parties. In addition, the implementation of secure network protocols, such as Transport Layer Security (TLS), for communications between nodes can help prevent data interception. The use of anomaly detection mechanisms is also a solution for monitoring and detecting suspicious activity or unusual traffic patterns that could indicate a routing attack. Furthermore, diversifying data transmission paths and decentralizing network infrastructure can reduce reliance on specific paths, thus minimizing the risk of interception. These strategies enhance the security of blockchain networks in copyright management by ensuring data confidentiality, integrity, and protection against malicious interference [56] [57].

Preventing the double spending attack: a double-spending attack, where an attacker spends the same cryptocurrency or token twice by altering blockchain transaction history, can be prevented with robust consensus mechanisms like Proof of Work (PoW) or PoS. These mechanisms effectively guarantee that only one version of the truth (the longest or most valid chain) is accepted on the network. The implementation of real-time transaction verifications and multiple confirmations for each transaction can also significantly reduce the risk of double spending. This means that a transaction is only considered valid once it has been confirmed by a sufficient number of nodes on the network. Additionally, the constant monitoring of the network is crucial for detecting anomalies and double-spending attempts at an early stage, where network nodes must be able to detect and reject fraudulent transactions, thus preventing them from being recorded in the blockchain. Finally, in systems based on the mechanism PoS, malicious parties risk losing their stake (the tokens they have staked) if they attempt to carry out double-spending attacks, adding an extra layer of deterrence [58].

Preventing from smart contract vulnerabilities: smart contract vulnerabilities, often due to code flaws, logic errors, or unexpected interactions with other contracts, require rigorous prevention by examining and auditing the code by blockchain security experts. This involves static and dynamic code analysis, checking for known vulnerabilities, and evaluating the logic of the contracts to identify potential flaws. It is also important to implement good development practices, like defensive programming, extensive unit testing, and security mechanisms such as transaction locks and limits, to reinforce smart contract robustness. Additionally, implementing procedures for managing security updates and corrections is effective, as it ensures rapid updates or corrections to smart contracts upon the discovery of vulnerabilities, without compromising operational continuity or data security. Finally, in order to prevent vulnerabilities right from the design phase, developers should be trained in optimal security practices for smart contract creation. All the aforementioned methods aim to ensure that blockchain-based copyright management applications are safeguarded against smart contract vulnerabilities, thereby securing the integrity, security, and reliability of transactions and records in these systems [6] [59] [60].

VI. Conclusion

Blockchain technology represents a transformative force for addressing the security challenges inherent in the copyright management sector. In this paper, we examined the various security vulnerabilities in the four main copyright management applications and illustrated the effectiveness of blockchain technology in addressing these issues. We also discussed the various strategies appropriate for mitigating the most common attacks on blockchain technology in the context of copyright management applications if these latter are blockchain-based.

References

[1] Zhiyong Zhang. Security, trust and risk in digital rights management ecosystem. *2010 International Conference on High Performance Computing & Simulation, IEEE*, pages 498–503, 2010.

[2] Alexander Savelyev. Copyright in the blockchain era: Promises and challenges. *Computer law & security review, Elsevier*, 34(3):550–561, 2018.

[3] Konstantinos Charmanas, Nikolaos Mittas, and Lefteris Angelis. Topic and influence analysis on technological patents related to security vulnerabilities. *Computers & Security, Elsevier*, 128:103128, 2023.

[4] Nour El Madhoun, Julien Hatin, and Emmanuel Bertin. A decision tree for building it applications. *Annals of Telecommunications*, 76(3):131–144, 2021.

[5] Kathleen Bridget Wilson, Adam Karg, and Hadi Ghaderi. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. *Business Horizons, Elsevier*, 65(5):657–670, 2022.

[6] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. Smart contract: Attacks and protections. *IEEE Access*, 8:24416–24427, 2020.

[7] Zulfiqar Ali Khan and Akbar Siami Namin. Ethereum smart contracts: Vulnerabilities and their classifications. *2020 IEEE International Conference on Big Data (Big Data), IEEE*, pages 1–10, 2020.

[8] Kevin Daimi, Ioanna Dionysiou, and Nour El Madhoun. *Principles and Practice of Blockchains*. Springer Nature, 2022.

[9] Shreshta Kaushik and Nour El Madhoun. Analysis of blockchain security: Classic attacks, cybercrime and penetration testing. *MobiSecServ 2023 (The Eighth International Conference On Mobile And Secure Services), IEEE*, 2023.

[10] Yuanjun Ding, Li Yang, Wenfeng Shi, and Xuliang Duan. The digital copyright management system based on blockchain. *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), IEEE*, pages 63–68, 2019.

[11] Sijia Zhao and Donal O'Mahony. Bmcprotector: A blockchain and smart contract based application for music copyright protection. *Proceedings of the 2018 International Conference on Blockchain Technology and Application*, pages 1–5, 2018.

[12] Joshua B Powers. Patents and royalties. *Privatization and public universities, Indiana University Press Bloomington*, pages 129–150, 2006.

[13] Jhonny Antonio Cadavid. The origin and purpose of legal protection for the integrity of copyright metadata. *IIC-International Review of Intellectual Property and Competition Law, Springer*, 54(8):1179–1202, 2023.

[14] Su Yeon Esther Jeong. Value of nfts in the digital art sector and its market research. *Sotheby's Institute of Art-New York*, 2022.

[15] Christopher Sprigman. Reform (aliz) ing copyright. *Intellectual Property Law and History, Routledge*, pages 277–360, 2017.

[16] Seyed Mojtaba Hosseini Bamakan, Nasim Nezhadsistani, Omid Bodaghi, and Qiang Qu. Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. *Scientific Reports, Nature Publishing Group UK London*, 12(1):2178, 2022.

[17] Véronique Pouillard. Intellectual property rights and country-of-origin labels in the luxury industry. *The Oxford Handbook of Luxury Business, Oxford University Press Oxford*, 2020.

[18] Frédérick Lamare and Aurélien Portelli. The use of records to manage risks associated with the decommissioning of nuclear facilities. *Proceedings of the 29th European Safety and Reliability Conference, European Safety and Reliability Conference (ESREL)*, pages 3874–3881, 2019.

[19] Ruth Towse. Economics of copyright collecting societies and digital rights: is there a case for a centralised digital copyright exchange? *Review of economic research on copyright issues*, 9(2):3–30, 2012.

[20] Rebecca Tushnet. All of this has happened before and all of this will happen again: Innovation in copyright licensing. *Berkeley technology law journal, JSTOR*, 29(3):1447–1488, 2015.

[21] Paweł Kossecki and Oguzhan Akin. Valuation of copyrights to audiovisual works: transparency practices of the copyright management organizations in the european union. *Ekonomia i Prawo. Economics and Law*, 20(3):543–571, 2021.

[22] Arista Szu-Yu Kuo. Professional realities of the subtitling industry: The subtitlers' perspective. *Audiovisual translation in a global context: Mapping an ever-changing landscape, Springer*, pages 163–191, 2015.

[23] Theo Papadopoulos. The economics of copyright, parallel imports and piracy in the music recording industry. *PhD Thesis, Victoria University*, 2002.

[24] David Megías, Minoru Kuribayashi, and Amna Qureshi. Survey on decentralized fingerprinting solutions: Copyright protection through piracy tracing. *Computers, MDPI*, 9(2):26, 2020.

[25] Peng Zhu, Jian Hu, Xiaotong Li, and Qingyun Zhu. Using blockchain technology to enhance the traceability of original achievements. *IEEE Transactions on Engineering Management*, 2021.

[26] Alastair Dunning. Tracing copyright holders: How two digitisation projects coped with copyright for historical material. 2004.

[27] Vicki Oliveri, Glenn Porter, Chris Davies, and Pamela James. Art crime: the challenges of provenance, law and ethics. *Museum Management and Curatorship, Taylor & Francis*, 37(2):179–195, 2022.

[28] Alexandra Luzan. Art provenance yesterday, today, and tomorrow with a particular focus on blockchain technology. *Università Ca'Foscari Venezia*, 2023.

[29] Françoise Benhamou and Victor Ginsburgh. Copies of artworks: the case of paintings and prints. *Handbook of the Economics of Art and Culture, Elsevier*, 1:253–283, 2006.

[30] Rachel O'Dwyer. Limited edition: Producing artificial scarcity for digital art on the blockchain and its implications for the cultural industries. *Convergence, SAGE Publications Sage UK: London, England*, 26(4):874–894, 2020.

[31] Melanie Swan. Blockchain: Blueprint for a new economy. *" O'Reilly Media, Inc."*, 2015.

[32] Thiago Negrão Chuba and Gabriela Simões Pazelli. A new panorama for intellectual property: The benefits and challenges of blockchain. *Available at SSRN 4579686*, 2023.

[33] Stef Van Gompel. Copyright formalities in the internet age: Filters of protection or facilitators of licensing. *Berkeley Technology Law Journal, JSTOR*, 28(3):1425–1458, 2013.

[34] William S Strong. The copyright book: a practical guide. 2014.

[35] Pedro Letai. Don't think twice, it's all right: Towards a new copyright protection system. *INTERNATIONAL INTERDISCIPLINARY BUSINESS-ECONOMICS ADVANCEMENT CONFERENCE*, page 105, 2014.

[36] Jacques Derrida. Copy, archive, signature: a conversation on photography. 2010.

[37] Deanna Fong. Tales of the tape: The ontological, discursive, and ethical lives of literary audio artifacts. *Simon Fraser University*, 2019.

[38] Dhyey Mehta, Sudeep Tanwar, Umesh Bodkhe, Arpit Shukla, and Neeraj Kumar. Blockchain-based royalty contract transactions scheme for industry 4.0 supply-chain management. *Information processing & management, Elsevier*, 58(4):102586, 2021.

[39] Jiarui Liu. Blockchain copyright exchange-a prototype. *Buff. L. Rev., HeinOnline*, 69:1021, 2021.

[40] Sebastian Pech. Copyright unchained: how blockchain technology can change the administration and distribution of copyright protected works. *Nw. J. Tech. & Intell. Prop., HeinOnline*, 18:1, 2020.

[41] Tao Jiang, Aina Sui, Weiguo Lin, and Pengbin Han. Research on the application of blockchain in copyright protection. *2020 International Conference on Culture-oriented Science & Technology (ICCST), IEEE*, pages 616–621, 2020.

[42] Martin Zeilinger. Digital art as 'monetised graphics': Enforcing intellectual property on the blockchain. *Philosophy & Technology, Springer*, 31(1):15–41, 2018.

[43] Andres Guadamuz. The treachery of images: non-fungible tokens and copyright. *Journal Of Intellectual Property Law and Practice, Oxford University Press UK*, 16(12):1367–1385, 2021.

[44] John Quinn and Barry Connolly. Distributed ledger technology and property registers: displacement or status quo. *Law, Innovation and Technology, Taylor & Francis*, 13(2):377–397, 2021.

[45] Beniamin A Shakhnazarov. Lex registrum as a system of regulation of cross-border relations aimed at protection of intellectual property implemented by means of blockchain technology. *Kutafin Law Review*, 9(2):195–226, 2022.

[46] Tom W Bell. Copyrights, privacy, and the blockchain. *Ohio NUL Rev., HeinOnline*, 42:439, 2015.

[47] Abhinaw Sai Erri Pradeep, Robert Amor, and Tak Wing Yiu. Blockchain improving trust in bim data exchange: a case study on bimchain. *Construction Research Congress 2020, American Society of Civil Engineers Reston, VA*, pages 1174–1183, 2020.

[48] Kervins Nicolas, Yi Wang, George C Giakos, Bingyang Wei, and Hongda Shen. Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. *IEEE Access*, 9:3838–3857, 2020.

[49] Shubhani Aggarwal and Neeraj Kumar. Attacks on blockchain. *Advances in computers, Elsevier*, 121:399–410, 2021.

[50] Abhishek Guru, Bhabendu Kumar Mohanta, Hitesh Mohapatra, Fadi Al-Turjman, Chadi Altrjman, and Arvind Yadav. A survey on consensus protocols and attacks on blockchain technology. *Applied Sciences, MDPI*, 13(4):2604, 2023.

[51] Nan Jing, Qi Liu, and Vijayan Sugumaran. A blockchain-based code copyright management system. *Information Processing & Management, Elsevier*, 58(3):102518, 2021.

[52] Amna Qureshi and David Megías Jiménez. Blockchain-based multimedia content protection: Review and open challenges. *Applied Sciences, MDPI*, 11(1):1, 2020.

[53] Pim Otte, Martijn de Vos, and Johan Pouwelse. Trustchain: A sybil-resistant scalable blockchain. *Future Generation Computer Systems*, 107:770–780, 2020.

[54] Mubashar Iqbal and Raimundas Matulevičius. Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, 9:76153–76177, 2021.

[55] Tayebeh Rajabi, Alvi Ataur Khalil, Mohammad Hossein Manshaei, Mohammad Ashiqur Rahman, Mohammad Dakhilalian, Maurice Ngouen, Murtuza Jadliwala, and A Selcuk Uluagac. Feasibility analysis for sybil attacks in shard-based permissionless blockchains. *Distributed Ledger Technologies: Research and Practice, ACM New York, NY*, 2023.

[56] Gholamreza Ramezan, Cyril Leung, et al. A blockchain-based contractual routing protocol for the internet of things using smart contracts. *Wireless Communications and Mobile Computing, Hindawi*, 2018, 2018.

[57] Yujuan Wen, Fengyuan Lu, Yufei Liu, and Xinli Huang. Attacks and countermeasures on blockchains: A survey from layering perspective. *Computer Networks, Elsevier*, 191:107978, 2021.

[58] Xiaohu Chen, Anjia Yang, Jian Weng, Yao Tong, Cheng Huang, and Tao Li. A blockchain-based copyright protection scheme with proactive defense. *IEEE Transactions on Services Computing*, 2023.

[59] Jaturong Kongmanee, Phongphun Kijsanayothin, and Rattikorn Hewett. Securing smart contracts in blockchain. *2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW), IEEE*, pages 69–76, 2019.

[60] Yun Zhang, Zhi Tang, Jing Huang, Yue Ding, Hao He, Xiaosheng Xia, and Chunhua Li. A decentralized model for spatial data digital rights management. *ISPRS International Journal of Geo-Information, MDPI*, 9(2):84, 2020.